FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* v. JEFFREY BRIAN ZIEGLER, *Defendant-Appellant.*	No. 05-30177 D.C. No. CR-03-00008-RFC ORDER AND OPINION

Appeal from the United States District Court
for the District of Montana
Richard F. Cebull, District Judge, Presiding

Argued and Submitted
March 6, 2006—Seattle, Washington

Filed January 30, 2007

Before: Diarmuid F. O'Scannlain, Barry G. Silverman, and Ronald M. Gould, Circuit Judges.

Opinion by Judge O'Scannlain

COUNSEL

David F. Ness, Assistant Federal Defender, Great Falls, Montana, argued the cause for the defendant-appellant. Anthony R. Gallagher, Federal Defender, District of Montana, was on the briefs.

Marcia Hurd, Assistant United States Attorney, Billings, Montana, argued the cause for the plaintiff-appellee. William W. Mercer, United States Attorney, District of Montana, was on the brief.

ORDER

The petition for panel rehearing is GRANTED. The opinion filed on August 8, 2006, is withdrawn. The superseding opinion will be filed concurrently with this order. Further petitions for rehearing or rehearing en banc may be filed.

OPINION

O'SCANNLAIN, Circuit Judge:

We must determine whether an employee has an expectation of privacy in his workplace computer sufficient to suppress images of child pornography sought to be admitted into evidence in a criminal prosecution. If there is such an expectation, we must determine whether the search in this case was reasonable under the narrow exceptions to the Fourth Amendment's warrant requirement.

I

A

Frontline Processing ("Frontline"), a company that services Internet merchants by processing on-line electronic payments, is located in Bozeman, Montana.[1] On January 30, 2001, Anthony Cochenour, the owner of Frontline's Internet-service provider and the fiancé of a Frontline employee, contacted Special Agent James A. Kennedy, Jr. of the FBI with a tip that a Frontline employee had accessed child-pornographic websites from a workplace computer.

---

[1]Although the district court referred to the company as "Front Line," we use the single-word formulation which more frequently appears in the record.

Agent Kennedy pursued the report that day, first contacting Frontline's Internet Technology ("IT") Administrator, John Softich. One of Softich's duties at Frontline was to monitor employee use of the workplace computers including their Internet access. He informed Kennedy that the company had in place a firewall, which permitted constant monitoring of the employees' Internet activities.[2]

During the interview, Softich confirmed Cochenour's report that a Frontline employee had accessed child pornography via the Internet. Softich also reported that he had personally viewed the sites and confirmed that they depicted "very, very young girls in various states of undress." Softich further informed Kennedy that, according to the Internet Protocol address and log-in information, the offending sites were accessed from a computer in the office of Appellant Jeffrey Brian Ziegler, who had been employed by Frontline as director of operations since August 2000. Softich also informed Kennedy that the IT department had already placed a monitor on Ziegler's computer to record its Internet traffic by copying its cache files.[3]

---

[2]A firewall is a piece of "computer hardware or software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outsider computer users (as of the Internet)." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 471 (11th ed. 2003). It can also be "programmed to analyze the network traffic flowing between [a] computer and the Internet"; it then "compares the information it monitors with a set of rules in its database," and "[i]f it sees something not allowed . . . the firewall can block and prevent the action." NEWTON'S TELECOM DICTIONARY 392 (22nd ed. 2006). Further, "[m]ost firewall programs let you adjust the rules to allow certain types of data to flow freely back and forth without interference." *Id.*

[3]A cache is "a computer memory with very short access time used for storage of frequently or recently used instructions or data." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 171 (11th ed. 2003). "[I]nformation is cached by placing it closer to the user or user application in order to make it more readily and speedily available . . . ." NEWTON'S TELECOM DICTIONARY 189 (22nd ed. 2006).

Agent Kennedy next interviewed William Schneider, Softich's subordinate in Frontline's IT department. Schneider confirmed that the IT department had placed a device in Ziegler's computer that would record his Internet activity. He reported that he had "spot checked" Ziegler's cache files and uncovered several images of child pornography. A review of Ziegler's "search engine cache information" also disclosed that he had searched for "things like 'preteen girls' and 'underage girls.' " Furthermore, according to Schneider, Frontline owned and routinely monitored all workplace computers. The employees were aware of the IT department's monitoring capabilities.

B

The parties dispute what happened next. According to testimony that Softich and Schneider provided to a federal grand jury, Agent Kennedy instructed them to make a copy of Ziegler's hard drive because he feared it might be tampered with before the FBI could make an arrest. Agent Kennedy, however, denied that he directed the Frontline employees to do anything. According to his testimony, his understanding was that the IT department had already made a backup copy of Ziegler's hard drive. As the government points out, his notes from the Softich interview say, "IT Dept has backed up JZ's hard drive to protect info." Thinking that the copy had already been made, Kennedy testified that he instructed Softich only to ensure that no one could tamper with the backup copy.

Whatever Agent Kennedy's actual instructions, the Frontline IT employees' subjective understanding of that conversation seems evident from their actions during the late evening of January 30, 2001. Around 10:00 p.m., Softich and Schneider obtained a key to Ziegler's private office from Ronald Reavis, the chief financial officer of Frontline, entered Ziegler's office, opened his computer's outer casing, and made two copies of the hard drive.

Shortly thereafter, Michael Freeman, Frontline's corporate counsel, contacted Agent Kennedy and informed him that Frontline would cooperate fully in the investigation. Freeman indicated that the company would voluntarily turn over Ziegler's computer to the FBI and thus explicitly suggested that a search warrant would be unnecessary.[4] On February 5, 2001, Reavis delivered to Agent Kennedy Ziegler's computer tower (containing the original hard drive) and one of the hard drive copies made by Schneider and Softich. Schneider delivered the second copy sometime later. Forensic examiners at the FBI discovered many images of child pornography.

C

On May 23, 2003, a federal grand jury handed down a three-count indictment charging Ziegler with receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2); possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B); and receipt of obscene material, in violation of 18 U.S.C. § 1462.[5] At arraignment, Ziegler entered a plea of not guilty.

Ziegler filed several pretrial motions. At issue here is Ziegler's April 23, 2004, motion to suppress the evidence obtained from the search of Ziegler's workplace computer. Ziegler argued that Agent Kennedy, lacking a warrant, violated the Fourth Amendment by directing the Frontline employees to enter his private office and to search his com-

[4]Agent Kennedy explained that this cooperation was the reason he did not pursue a search warrant. He testified, "At this point, counselor, everybody at Frontline Processing is telling me they're going to cooperate, so I'm not going to go in and start serving search warrants on a company if they're going to cooperate. I have no desire to do that."

[5]No explanation appears in the record for the two year, three month interval between delivery of the computer to the FBI and issuance of the indictment. In any event, Ziegler does not raise any issue regarding such delay.

puter. The government argued that the search was voluntary and therefore private in nature.

On August 10, 2004, the district court held a suppression hearing at which Agent Kennedy and Schneider testified.[6] Agent Kennedy, several times, denied that he instructed Softich and Schneider to make a copy of Ziegler's hard drive or to undertake any search in addition to what the employees had already done. Schneider, however, again testified that Kennedy directed him to make a copy of the hard drive. Schneider's account was also reflected in a time-line he had prepared for Kennedy.[7]

On September 8, 2004, the district court entered a written order denying Ziegler's motion to suppress. Importantly, the court made the factual finding that "Agent Kennedy contacted Softich and Schneider on January 30, 2001 and *directed them to make a back-up of Defendant's computer files*." (emphasis added). However, citing *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), the court ultimately held that Ziegler had

[6]The defense also offered the testimony of a computer forensics expert, but that testimony was not relevant to the motion to suppress.

[7]On appeal, the government attempts to reconcile the contradictory accounts of the January 30, 2001, interview as a case of simple miscommunication. It explains that confusion ensued when Schneider told Agent Kennedy that they were copying Ziegler's cache files onto a second hard drive. Kennedy, whom the government characterizes as not particularly tech-savvy, allegedly understood Schneider to mean that the IT department had already made a copy of Ziegler's entire hard drive. Thus, it suggests that Agent Kennedy's instructions were only that the IT employees should secure the copy he thought had *already* been made.

There is, in short, a factual dispute concerning the extent of the government's involvement in the search and a corresponding legal dispute as to whether that involvement implicates the Fourth Amendment. *See United States v. Miller*, 688 F.2d 652, 658 (9th Cir. 1982). However, we need not address these issues if Ziegler had no reasonable expectation of privacy in any place searched or any item seized. *See, e.g.*, *United States v. Wong*, 334 F.3d 831, 839 (9th Cir. 2003).

no reasonable expectation of privacy in "the files he accessed on the Internet" and therefore denied Ziegler's motion.

Ziegler subsequently entered into a written plea agreement with the government. Pursuant to the agreement, the government agreed to dismiss the child pornography counts in exchange for Ziegler's agreement to plead guilty to the receipt of obscene material. The parties conditioned the plea agreement on Ziegler's ability to appeal the district court's denial of the pretrial motions, including the motion to suppress. A change of plea hearing occurred on September 24, 2004.

On March 4, 2005, the district court sentenced Ziegler to a two-year term of probation and imposed a fine of $1,000. Ziegler timely filed a notice of appeal.

II

Ziegler's sole contention on appeal is that the January 30, 2001, entry into his private office to search his workplace computer violated the Fourth Amendment and, as such, the evidence contained on the computer's hard drive must be suppressed.[8]

A

Ziegler argues that "[t]he district court erred in its finding that Ziegler did not have a legitimate expectation of privacy in his office and computer." He likens the workplace computer to the desk drawer or file cabinet given Fourth Amendment protection in cases such as *O'Connor v. Ortega*, 480 U.S. 709 (1987). Ziegler further contends that the Fourth Circuit's *Simons* case is inapposite. Whereas in *Simons* "the person conducting the search was a network administrator whose purpose was to search for evidence of employee misconduct,"

[8]We review de novo the district court's denial of Ziegler's motion to suppress. *United States v. Noushfar*, 78 F.3d 1442, 1447 (9th Cir. 1996).

in this case "the search was conducted at the behest of Agent Kennedy who was undeniably seeking evidence of a crime."

The government, of course, views the matter quite differently. It contends that the district court's ruling was correct—Ziegler did not have an objectively reasonable expectation of privacy in his workplace computer. The government argues in its brief:

> Society could not deem objectively reasonable that privacy interest where an employee uses a computer paid for by the company; [sic] Internet access paid for by the company, in the company office where the company pays the rent . . . . This is certainly even more so true where the company has installed a firewall and a whole department of people whose job it was to monitor their employee's Internet activity.

As we know, the Fourth Amendment protects people, not places. *Katz v. United States*, 389 U.S. 347, 351 (1967). Although it is often true that "for most people, their computers are their most private spaces," *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting), the validity of that expectation depends entirely on its context. *Cf. Ortega*, 480 U.S. at 715 ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable.").

[1] In that vein, a criminal defendant may invoke the protections of the Fourth Amendment only if he can show that he had a *legitimate* expectation of privacy in the place searched or the item seized. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). This expectation is established where the claimant can show: (1) a subjective expectation of privacy; and (2) an objectively reasonable expectation of privacy. *See id.* (citing *Katz*, 389 U.S. at 351, 361); *United States v. Shryock*, 342 F.3d 948, 978 (9th Cir. 2003). It is Ziegler's burden to prove

both elements. *United States v. Caymen*, 404 F.3d 1196, 1199 (9th Cir. 2005) (citation omitted).

[2] The threshold question then is whether Ziegler had a legitimate expectation of privacy in the area searched or the object seized. If he had no such expectation, we need not consider whether the search was reasonable.

1

[3] The government does not contest Ziegler's claim that he had a subjective expectation of privacy in his office and the computer. The use of a password on his computer and the lock on his private office door are sufficient evidence of such expectation. *See United States v. Bailey*, 272 F. Supp. 2d 822, 835 (D. Neb. 2003) (citation omitted).

2

[4] But Ziegler's expectation of privacy in his office and workplace computer must also have been objectively reasonable. The seminal case addressing the reasonable expectations of private employees in the workplace is *Mancusi v. DeForte*, 392 U.S. 364 (1968). In *Mancusi*, the Supreme Court addressed whether a union employee had a legitimate expectation of privacy, and therefore Fourth Amendment standing, in the contents of records that he stored in an office that he shared with several other union officials. The Court held that DeForte had standing to object to the search and that the search was unreasonable, noting that it was clear that "if DeForte had occupied a 'private' office in the union headquarters, and union records had been seized from a desk or a filing cabinet in that office, he would have had standing." *Id.* at 369. That was so because he could expect that he would not be disturbed except by business or personal invitees and that the records would not be taken except with the permission of his supervisors. *Id.* The Court thought the fact that the office

was shared with a few other individuals to be of no constitutional distinction.

[5] *Mancusi* compels us to recognize that in the private employer context, employees retain at least some expectation of privacy in their offices. *Id. See also Ortega v. O'Connor*, 480 U.S. 709, 716 (1987) (noting that in *Mancusi* "this Court . . . recognized that employees may have a reasonable expectation of privacy against intrusions by police."); *id.* at 730 (Scalia, J., concurring) ("In *Mancusi v. DeForte*, we held that a union employee had Fourth Amendment rights with regard to an office at union headquarters that he shared with two other employees, even though we acknowledged that those other employees, their personal or business guests, and (implicitly) 'union higher-ups' could enter the office.") (internal citations omitted).

[6] Furthermore, Ziegler's expectation of privacy in his office was reasonable on the facts of this case. His office was not shared by co-workers, and kept locked. *See Schowengerdt v. United States*, 944 F.2d 483, 487 (9th Cir. 1991) ("Schowengerdt would enjoy a reasonable expectation of privacy in areas given over to his exclusive use, unless he was on notice from his [government] employer that searches of the type to which he was subjected might occur from time to time for work-related purposes."); *United States v. Taketa*, 923 F.2d 665, 672-73 (9th Cir. 1991). And while there was a master key, the existence of such will not necessarily defeat a reasonable expectation of privacy in an office given over for personal use. *See Taketa*, 923 F.2d at 673 (noting that allowing the existence of a master key to overcome the expectation of privacy would defeat the legitimate privacy interest of any hotel, office, or apartment occupant).

[7] Because Ziegler had a reasonable expectation of privacy

in his office, any search of that space and the items located therein must comply with the Fourth Amendment.[9]

III

[8] The next step is to inquire whether there was a search or seizure by the government. We need not dwell upon this matter too long. Given the district court's factual findings, we treat Softich and Schneider as de facto government agents. *See United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994). While the two Frontline employees may not have scoured the desk drawers and cabinets for evidence, as the agents did in *Mancusi*, 392 U.S. at 365, they undoubtedly "searched" Ziegler's office when they entered to make a copy of the hard drive of his computer. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 2.1(a) (4th ed. 2004) ("Under the traditional approach, the term 'search' is said to imply some exploratory investigation, or an invasion and quest, a looking for or seeking out.") (internal quotation omitted). The employees obtained a key in order to unlock the office, entered the office, copied Ziegler's hard drive, and left.

IV

A

[9] The remaining question is whether the search of Ziegler's office and the copying of his hard drive were "unreasonable" within the meaning of the Fourth Amendment. As in *Mancusi*, the government does not deny that the search and seizure were without a warrant, and "it is settled for purposes

[9]Had the company computer assigned to Ziegler for his business-use only been physically located outside a private office, we might have had to consider whether Ziegler had reasonable expectation of privacy in the device itself, in the face of a corporate policy of monitoring the corporate computers. *See Muick v. Glenayre Electronics*, 280 F. 3d 741, 743 (7th Cir. 2002). However, we leave that question for another day.

of the Amendment that 'except in certain carefully defined classes of cases, a search of private property without proper consent is 'unreasonable' unless it has been authorized by a valid search warrant.' " *Mancusi*, 392 U.S. at 370 (quoting *Camara v. Municipal Court*, 387 U.S. 523, 528-529 (1967)).

[10] One well-settled exception is where valid consent is obtained by the government. *Davis v. United States*, 328 U.S. 582, 593-594 (1946); *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). In proving voluntary consent, the government "is not limited to proof that consent was given by the defendant, but may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." *United States v. Matlock*, 415 U.S. 164, 171 (1974); *see also United States v. Davis*, 332 F.3d 1163, 1168-69 (9th Cir. 2003). Common authority to authorize a search rests upon the premise that one "[has] assumed the risk that one of [his] number might permit the common area to be searched." *Matlock*, 415 U.S. at 171 n. 7.

B

[11] We first consider whether Frontline exercised common authority over the office and the workplace computer such that it could validly consent to a search. *Mancusi* is again instructive. In *Mancusi*, the Supreme Court recognized that in his office, DeForte retained an expectation "that records would not be taken [by the police] except with his permission or that of his union superiors." 392 U.S. at 369. The Court continued: "It is, of course, irrelevant that the Union or some of its officials might validly have consented to a search of the area where the records were kept, regardless of DeForte's wishes, for it is not claimed that any such consent was given, either expressly or by implication." *Id.* at 369-70; *see also United States v. Carter*, 569 F.2d 801, 804 (4th Cir. 1978), *cert. denied* 435 U.S. 973 (1978). *Mancusi* thus establishes that even where a private employee retains an expectation that

his private office will not be the subject of an unreasonable government search, such interest may be subject to the possibility of an employer's consent to a search of the premises which it owns.

[12] We are also convinced that Frontline could give valid consent to a search of the contents of the hard drive of Ziegler's workplace computer because the computer is the type of workplace property that remains within the control of the employer "even if the employee has placed personal items in [it]." *Ortega*, 480 U.S. at 716. In *Ortega*, the Supreme Court offered an analogy that is helpful to our resolution of this question. *Ortega*, 480 U.S. at 716. The Court posited a situation where an employee brings a piece of personal luggage to work and places it within his office. The Court noted that "[w]hile . . . the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* of the luggage is not affected in the same way." *Id.* (emphasis in original). The Court further explained that "[t]he appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address." *Id.*

[13] The workplace computer, however, is quite different from the piece of personal luggage which the Court described in *Ortega*. Although use of each Frontline computer was subject to an individual log-in, Schneider and other IT-department employees "had complete administrative access to anybody's machine." The company had also installed a firewall, which, according to Schneider, is "a program that monitors Internet traffic . . . from within the organization to make sure nobody is visiting any sites that might be unprofessional." Monitoring was routine, and the IT department reviewed the log created by the firewall "[o]n a regular basis," sometimes daily if Internet traffic was high enough to warrant it. Finally, upon their hiring, Frontline employees were apprised of the company's monitoring efforts through training and an

employment manual, and they were told that the computers were company-owned and not to be used for activities of a personal nature.

[14] In this context, Ziegler could not reasonably have expected that the computer was his personal property, free from any type of control by his employer. The contents of his hard drive, like the files in *Mancusi*, 392 U.S. at 369, were work-related items that contained business information and which were provided to, or created by, the employee in the context of the business relationship. Ziegler's downloading of personal items to the computer did not destroy the employer's common authority. *Ortega*, 480 U.S. at 716. Thus, Frontline, as the employer, could consent to a search of the office and the computer that it provided to Ziegler for his work.

C

[15] The remaining question is, given Frontline's *ability* to consent to a search, did it consent to a search of the office and the computer. We conclude that it did. The exact type of employer consent that was absent in *Mancusi* clearly exists in this case. While the district court found that Softich and Schneider acted at the direction of Agent Kennedy, the record shows that Softich and Schneider received consent to search the office and the keys to the office from the Chief Financial Officer of Frontline Ronald Reavis. Schneider testified:

> [W]hen I returned from the meeting with Agent Kennedy, I spoke to John Softich, and then we, in turn, both went up and spoke to Ronald Reavis. Explained the situation to him. Said that, you know, [the FBI] wanted a backup made of this information, that we were going to do it sometime at night to make sure that we were undisturbed. And he said that as an officer of the company, he was okay with that, and he said that we could go forward and do that. He gave me his — a key to the building and to the

> offices, and then I came in sometime after 10 o'clock and did the copy.

In addition, Softich testified that Reavis had authorized them to make the copy of the hard drive. Softich was asked, "So Ron [Reavis] gave [Schneider] the key and said, Go do this?" Softich answered in the affirmative.

[16] This testimony makes clear that Ziegler's superiors at Frontline, in particular Reavis, an officer of the company, gave consent to a search of the property that the company owned and which was not of a personal nature.[10] *See United States v. Gargiso*, 456 F.2d 584, 586-87 (2d Cir. 1972) (upholding search where FBI agent received consent of highest-ranking corporate officer on the scene).

V

[17] Although Ziegler retained a legitimate expectation of privacy in his workplace office, Frontline retained the ability to consent to a search of Ziegler's office and his business computer. And because valid third party consent to search the office and computer located therein was given by his employer, the district court's order denying suppression of the evidence of child pornography existing on Ziegler's computer is

AFFIRMED.

[10]Here, the Frontline employees may have felt under some pressure to cooperate with Agent Kennedy, but "this alone does not render [the employees'] behavior involuntary." *United States v. Black*, 767 F.2d 1334, 1339 (9th Cir. 1985). Moreover, it does not matter that Chris Kittner, the owner of Frontline and a personal friend to Ziegler, objected (in some vague sense) to cooperation with the authorities. Reavis, a corporate officer with a key to Ziegler's office, did consent to the search. *See United States v. Sherwin*, 539 F.2d 1, 7-8 (9th Cir. 1976).